RECENT SAFETY ASSESSMENT PROCESS ACTIVITIES

James Treacy
National Resource Specialist- Avionics
Phone: (425) 227-2760
Fax: (425) 227-1181
e:mail: james.treacy@faa.gov

OBJECTIVE

- PROVIDE INFORMATION ON LATEST DEVELOPMENTS
- PROVIDE REFERENCES FOR FUTURE USE
- OVERVIEW ONLY
  - LIMITED DETAILS
  - NOT INSTANT EXPERTS

OUTLINE

- SAE ARPs
  - ARP 4754
  - ARP 4761
- 25.1309
  - RULE CHANGE
  - ADVISORY CHANGE

PREVIOUS SAFETY ASSESSMENT GUIDANCE

- SAE ARP 926A (1979)
  - PIECE-PART FAILURE MODES AND EFFECTS ANALYSIS (FMEA) AND FAULT TREE ANALYSIS
- SAE ARP 1834 (1986)
  - FAULT AND FAILURE ANALYSIS FOR DIGITAL SYSTEMS

PREVIOUS SAFETY ASSESSMENT GUIDANCE

- PROBLEMS WITH ARP 926A AND ARP 1834
  - GUIDANCE NOT COMPLETE FOR SAFETY PURPOSES
  - ADDRESSED RELIABILITY/MAINTAINABILITY
  - OUTDATED
    - DID NOT FIT WITH DO-178B
    - DID NOT ADDRESS AIRCRAFT LEVEL ANALYSIS
    - DID NOT ADEQUATELY COVER COMMON MODE ANALYSIS
    - NO PRELIMINARY SYSTEM SAFETY ASSESSMENT (PSSA)

RESOLUTION

- ARP 4754 AND ARP 4761 CREATED
- ARP 926A AND ARP 1834 REVISED BY SAE SUB-COMMITTEE S-18 TO INCLUDE A NOTE THAT INDICATES FOR AEROSPACE APPLICATIONS THESE AEROSPACE RECOMMENDED PRACTICES ARE OBSOLETE AND HAVE BEEN SUPERSEDED BY ARP 4761

ARP 4754

- "CERTIFICATION CONSIDERATIONS FOR HIGHLY INTEGRATED OR COMPLEX AIRCRAFT SYSTEMS"
  - DESCRIBES THE AIRCRAFT SYSTEMS ENGINEERING PROCESS
    - REQUIREMENTS CAPTURE
    - ALLOCATION OF REQUIREMENTS
    - ARCHITECTURAL CONSIDERATIONS
    - SOFTWARE LEVEL DETERMINATION
    - INTEGRATION

ARP 4754

- SAFETY ASSESSMENT PROCESS (HIGH LEVEL)
  - FUNCTIONAL HAZARD ASSESSMENT (FHA)
  - PRELIMINARY SYSTEM SAFETY ASSESSMENT (PSSA)
  - SYSTEM SAFETY ASSESSMENT (SSA)
- REQUIREMENTS VALIDATION
- SYSTEM VERIFICATION

ARP 4761

- "GUIDELINES AND METHODS OF PERFORMING THE SAFETY ASSESSMENT PROCESS ON CIVIL AIRBORNE SYSTEMS AND EQUIPMENT"
  - DESCRIBES THE PROCESS IN DETAIL
    - FUNCTIONAL HAZARD ASSESSMENT (FHA)
    - PRELIMINARY SYSTEM SAFETY ASSESSMENT (PSSA)
    - SYSTEM SAFETY ASSESSMENT (SSA)
  - REPLACES ARP 926A AND ARP 1834 FOR PURPOSES OF SAFETY

ARP 4761

- NEW CONCEPTS
  - MORE FORMAL DESCRIPTION OF *COMMON CAUSE ANALYSIS*
  - DIVIDED INTO THREE AREAS OF STUDY
    - ZONAL SAFETY ANALYSIS
    - PARTICULAR RISKS ANALYSIS
    - COMMON MODE ANALYSIS

ARP 4761

- NEW CONCEPTS
  - *AIRCRAFT* LEVEL FUNCTIONAL HAZARD ASSESSMENT
  - PRELIMINARY SYSTEM SAFETY ASSESSMENT
    - PROVIDES A MORE SYSTEMATIC MEANS OF EVALUATING SAFETY EARLY IN THE DESIGN PROCESS AND TO REDUCE SURPRISES AT THE END OF THE DEVELOPMENT PROGRAM.

ARP 4761

- NEW CONCEPTS
  - FAULT TREE ANALYSES
    - PROBABILITY CALCULATIONS OF THE FAILURE CONDITION BASED ON A PER FLIGHT BASIS
    - PROBABILITY PER FLIGHT HOUR DETERMINED BY DIVIDING RESULT BY AVERAGE FLIGHT TIME FOR THE PARTICULAR MODEL AIRCRAFT
    - EXPOSURE TIME FOR LATENT FAILURES IS RESOLVED AND OTHER CASES OF MONITORED FAILURES WITH IMPERFECT MONITORS ARE EXPLAINED

ARP 4761

- GOOD ORGANIZATION COMPENSATES FOR INTIMIDATING SIZE
  - BASIC TEXT: APPROX 30 PAGE OVERVIEW
  - SEVERAL APPENDICES, ONE DEVOTED TO EACH TOOL
    - FHA
    - PSSA
    - SSA
      - FMEA
      - FTA
    - CCA
    - (etc.)
  - LAST APPENDIX IS CONTIGUOUS EXAMPLE

ARP 4761 CAUTION

- ARP 4761 REPRESENTS A CONSENSUS OF BEST PRACTICE(S)
- TECHNIQUES HAVE NOT BEEN USED IN THEIR ENTIRETY BY ANY ONE MANUFACTURER
- GRADUAL IMPLEMENTATION OVER TIME
- EXISTING METHODS ACCEPTABLE IF:
  - INTENT OF THE SAFETY ANALYSIS IS MET
    - MAY NEED SOME ADDITIONAL ANALYSIS IF EXISTING METHOD INSUFFICIENT IN SOME AREA(S)
- EXCELLENT RESOURCE FOR APPLICANTS WITH LIMITED EXPERIENCE IN THIS AREA

ARP STATUS

- THE SOCIETY OF AUTOMOTIVE ENGINEERS (SAE) APPROVED AND PUBLISHED ARP 4761 IN NOVEMBER 1996.
- ARP 4754 WAS APPROVED AND PUBLISHED IN DECEMBER 1996.
- COPIES OF THESE DOCUMENTS ARE AVAILABLE FROM SAE
  - APPROX $52.00 EACH.

25.1309

- RULE EVOLUTION
- AC EVOLUTION
- SD&A HWG
  - RULE(S) & AC CHANGE
  - CHANGES
    - POWERPLANTS
  - STATUS

BRIEF HISTORY
EVOLUTION OF § 25.1309

- NO AMDT 2/1/65
  - FROM CAR 4b.606
  - "NO SINGLE FAILURE . . ." (PLUS LATENTS)
- AMDT 25-23 5/8/70
  - "INVERSE RELATIONSHIP" PHILOSOPHY
  - ALERT CREW TO UNSAFE SYSTEM OPER COND
- AMDT 25-41 9/1/77
  - REDUCED CONSIDERATION SCOPE
- AMDT 25-xx ?/?/??
  - Returned to ARAC for more work

BRIEF HISTORY
EVOLUTION OF AC 25.1309

- AC 25.1309-1 9/7/82
- AC 25.1309-1A 6/21/88
- *AC 25.1309-1B DELAYED*

NOTE: FIRST ADVISORY CAME 12 YEARS AFTER "INVERSE RELATIONSHIP" PHILOSOPHY INTRODUCED

BRIEF HISTORY
WHAT CHANGED PHILOSOPHICALLY

- "NO AMDT" ASSUMPTIONS
  - MORE THAN ONE FAILURE - SAFE ENOUGH
    - (PLUS LATENTS)
    - QUESTIONABLE VALIDITY FOR ADVANCING TECHNOLOGY SYSTEMS/EQUIP
- AMDT 25-23 & LATER
  - "INVERSE RELATIONSHIP" PHILOSOPHY

COMMITEE ACTIVITY

- AVIATION RULEMAKING ADVISORY COMMITTEE (ARAC) WORKING GROUPS
  - REVISE AND HARMONIZE § /JAR 25.1309 AND 25.901 AND ASSOCIATED ADVISORY MATERIAL
    - HARMONIZE FAR WITH JAR
    - HARMONIZE SUPART E WITH SUBPART F
      - ON THIS SUBJECT
  - INTENT IS TO APPLY THE REQUIREMENTS OF REVISED § /JAR 25.1309 TO BOTH SUBPART E AND SUBPART F WITH SOME EXCEPTIONS

COMMITEE ACTIVITY

- THE ARAC *POWERPLANT INSTALLATIONS* HARMONIZATION WORKING GROUP PROPOSED:
  - CHANGES TO § /JAR 25.901(C) WHICH WOULD BE REVISED TO ESTABLISH A GENERAL REQUIREMENT FOR A POWERPLANT SAFETY ASSESSMENT AND WOULD APPLY THE REQUIREMENTS OF § /JAR 25.1309 TO POWERPLANT INSTALLATIONS EXCEPT, THE REQUIREMENTS OF § /JAR 25.1309(B) WOULD NOT APPLY TO:
  - THE EFFECTS OF AN ENGINE CASE BURN THROUGH OR RUPTURE
    - UNCONTAINED ENGINE ROTOR FAILURE
    - PROPELLER DEBRIS RELEASE
  - A NEW COMMON § /JAR ADVISORY CIRCULAR/ADVISORY MATERIAL JOINT, SAFETY ASSESSMENT OF POWERPLANT INSTALLATIONS, NO. 25.901(C)

COMMITEE ACTIVITY

- THE ARAC *SYSTEMS DESIGN & ANALYSIS* HARMONIZATION WORKING GROUP PROPOSED:
  - CHANGES TO BOTH 25.1301 AND 25.1309
  - A NEW 25.1310
  - A COMMON § /JAR ADVISORY CIRCULAR/ADVISORY MATERIAL JOINT FOR § /JAR 25.1309
    - THE SYSTEMS DESIGN & ANALYSIS HARMONIZATION WORKING GROUP IS PROPOSING TO DEFER WORK ON THE FOLLOWING ISSUES:
      - SOME ISSUES ON SPECIFIC RISK
      - SOME ISSUES ON TIME LIMITED DISPATCH FOR AIRPLANE SYSTEMS
  - PROPOSED REGULATORY CHANGES INCLUDE:
      - A REVISED 25.1301 WHICH WOULD PERMIT SYSTEMS WHICH DO NOT AFFECT SAFETY TO BE INSTALLED, EVEN IF THEY DO NOT PERFORM THEIR INTENDED FUNCTION.

CHANGES TO § 25.1309

- REVISIONS TO § 25.1309:
  - REQUIRE SAFETY RELATED SYSTEMS TO FUNCTION PROPERLY UNDER ANY OPERATIONAL OR ENVIRONMENTAL CONDITION APPROVED FOR THE AIRPLANE
  - REQUIRE THAT CATASTROPHIC FAILURE CONDITIONS BE EXTREMELY IMPROBABLE *AND* NOT RESULT FROM A SINGLE FAILURE.
  - REQUIRE THAT HAZARDOUS FAILURE CONDITIONS BE EXTREMELY REMOTE.
  - REQUIRE THAT MAJOR FAILURE CONDITIONS BE REMOTE.
  - ESTABLISH A NEW SECTION 25.1310 TO CONTAIN THE POWER DISTRIBUTION REQUIREMENTS NOW FOUND IN 25.1309.
  - DELETE THE ANALYSIS REQUIREMENTS OF 25.1309 FROM THE RULE.
    - THE ANALYSIS REQUIREMENTS HAVE BEEN ADDED TO THE ADVISORY CIRCULAR AND EXTENDED TO INCLUDE DESIGN ERRORS.
  - DESCRIBES EXPLICITLY THE SECTIONS TO WHICH 25.1309 APPLIES.
  - EXPLICITLY IDENTIFY BY SECTION THE REGULATIONS TO WHICH 25.1309 DOES NOT APPLY.

CHANGES TO § 25.1309

- § 25.1309 APPLICABILITY CLARIFICATIONS
  - § 25.1309 DOES NOT APPLY TO THE PERFORMANCE AND FLIGHT CHARACTERISTIC REQUIREMENTS OF SUBPART B AND THE STRUCTURAL REQUIREMENTS OF SUBPARTS C AND D, IT DOES APPLY TO ANY SYSTEM ON WHICH COMPLIANCE WITH ANY OF THOSE REQUIREMENTS IS DEPENDENT.
  - FLIGHT CONTROLS- CERTAIN SINGLE FAILURES OR JAMS COVERED BY § 25.671(c)(1) AND § 25.671(c)(3) ARE EXCEPTED FROM THE REQUIREMENTS OF § 25.1309(b)(1)(ii).
  - WHEEL BRAKES- CERTAIN SINGLE FAILURES COVERED BY § 25.735(b)(1) ARE EXCEPTED FROM THE REQUIREMENTS OF § 25.1309(b).
  - EMERGENCY EVACUATION PROVISIONS-THE FAILURE EFFECTS COVERED BY § 25.810(a)(1)(v) AND § 25.812 ARE EXCEPTED FROM THE REQUIREMENTS OF § 25.1309(b).
  - THE REQUIREMENTS OF § 25.1309(b) APPLY TO POWER PLANT INSTALLATIONS AS SPECIFIED IN § 25.901(c).

RELATIONSHIP OF § 25.1309 TO ARP 4761 AND ARP 4754

- THE FAA TRANSPORT AIRPLANE DIRECTORATE HAS RECOGNIZED THE TECHNIQUES OF SOCIETY OF AUTOMOTIVE ENGINEERS AEROSPACE RECOMMENDED PRACTICE DOCUMENTS ARP 4754 AND ARP 4761 AS AN ACCEPTABLE MEANS OF COMPLIANCE WITH THE REQUIREMENTS OF 25.1309, FOR THE SUBJECTS THEY COVER, IN A 1998 POLICY LETTER.
- THE FAA INTENDS TO RECOGNIZE THESE TECHNIQUES AS AN ACCEPTABLE MEANS OF COMPLIANCE FOR THE SUBJECTS THEY COVER, BUT NOT THE ONLY MEANS OF COMPLIANCE, IN ADVISORY CIRCULAR 25.1309-1B, WHEN IT IS EVENTUALLY ISSUED.

ARAC HWG STATUS

- THE ARAC POWERPLANT INSTALLATION HWG COMPLETED ITS WORK ON §25.901(C) AND THE ASSOCIATED AC ON JULY 24, 1998.

ARAC HWG STATUS

- THE ARAC SYSTEMS DESIGN AND ANALYSIS HWG HELD ITS “LAST” MEETING ON APRIL 23, 1998.
- ONE ISSUE TECHNICAL ISSUE IS UNRESOLVED.
  - FAA PROPULSION ENGINEERS TRADITIONALLY ASSUME THAT ANY LATENT FAILURE WILL OCCUR AND CONDUCT AN ANALYSIS TO DETERMINE IF THE NEXT FAILURE WILL RESULT IN A HAZARDOUS OR CATASTROPHIC FAILURE CONDITION. SINCE THIS IS NOT DONE FOR SYSTEMS, THIS ISSUE NEEDS TO BE RESOLVED PRIOR TO PUBLICATION OF AC 25.1309-1B.

ARAC HWG STATUS

- LATEST WORD
  - ADDITIONAL ISSUES HAVE BEEN RAISED BY THE ACTIONS OF OTHER HARMONIZATION EFFORTS AND BY THE FAA GENERAL COUNSEL INCLUDING:
  - THE APPLICATION OF THE PROPOSED 25.1309 TO FAILURE OF POWERED FLIGHT CONTROLS, BUT NOT TO FLIGHT CONTROL SYSTEM JAMS.
  - A REQUIREMENT THAT MINOR FAILURE CONDITIONS BE INFREQUENT, WITH A DEFIINITION FOR INFREQUENT.
  - A REQUIREMENT THAT SAFETY RELATED SYSTEMS, EQUIPMENT AND INSTALLATIONS OPERATE WITHOUT FAILURE FOR FREQUENTLY ENCOUNTERED OPERATING AND ENVIRONMENTAL CONDITIONS.
  - ELIZABETH ERICSON, DIRECTOR OF THE AIRCRAFT CERTIFICATION SERVICE HAS DECIDED TO SEND THE PROPOSED 25.1309 RULEMAKING PACKAGE BACK TO ARAC TO WORK ON THE OPEN ISSUES.

AC/AMJ 25.1309-1B

- CHANGES INCLUDE
  - REVISED DEFINITIONS FOR FAILURE CONDITIONS AND PROBABILITY
  - REVISED CRITERIA FOR WARNING, CAUTION AND ADVISORY INDICATION
  - A DEFINED METHOD FOR CALCULATING AVERAGE PROBABILITY
  - A NEW APPENDIX TO PERMIT THE NUMERICAL PROBABILITY CALCULATIONS TO
    - INCLUDE THE PROBABILITY OF CERTAIN ENVIRONMENTAL AND OPERATING CONDITIONS
    - CRITERIA FOR USE OF SYSTEM ARCHITECTURE TO REDUCE DEVELOPMENT ASSURANCE REQUIREMENTS

Relationship Between Probability and Severity of Failure Condition
DRAFT AC 25.1309-1B.

	NO SAFETY EFFECT
Effect on Airplane	No effect on operational capabilities or safety
Effect on Occupants	Inconvenience for passengers
Effect on Flight Crew	No effect on flight crew
Qualitative Probability	No Probability Requirement
Quantitative Probability	No Probability Requirement

DRAFT AC 25.1309-1B.

	MINOR
Effect on Airplane	Slight reduction in functional capabilities or safety margins
Effect on Occupants	Physical discomfort for passengers
Effect on Flight Crew	Slight increase in workload or use of emergency procedures
Qualitative Probability	Probable
Quantitative Probability	$< 1.0 \times 10^{-3}$ per flight hour Note 1

DRAFT AC 25.1309-1B.

	MAJOR
Effect on Airplane	Significant reduction in functional capabilities or safety margins
Effect on Occupants	Physical distress to passengers, possibly including injuries
Effect on Flight Crew	Physical discomfort or a significant increase in workload
Qualitative Probability	Remote
Quantitative Probability	$< 1.0 \times 10^{-5}$ per flight hour

DRAFT AC 25.1309-1B.

	HAZARDOUS
Effect on Airplane	Large reduction in functional capabilities or safety margins
Effect on Occupants	Serious or fatal injury to a small number of occupants
Effect on Flight Crew	Physical distress or excessive workload impairs ability to perform tasks
Qualitative Probability	Extremely Remote
Quantitative Probability	$< 1.0 \times 10^{-7}$ per flight hour

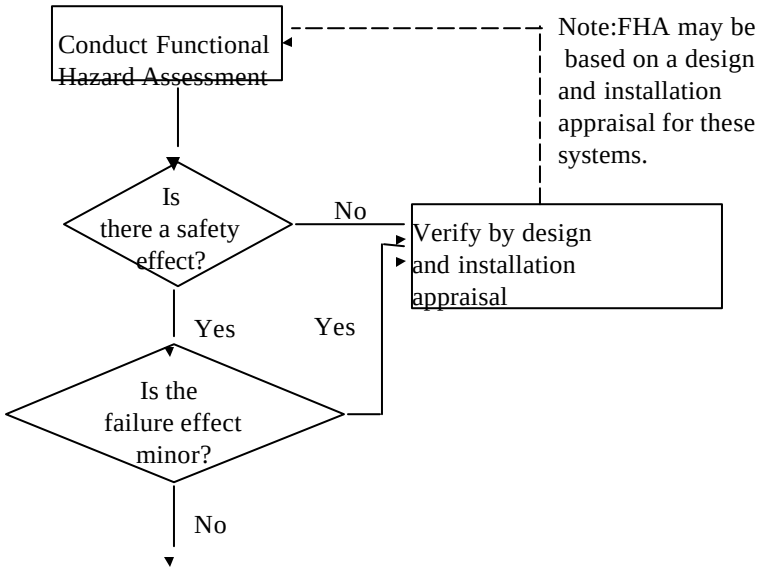
DRAFT AC 25.1309-1B.

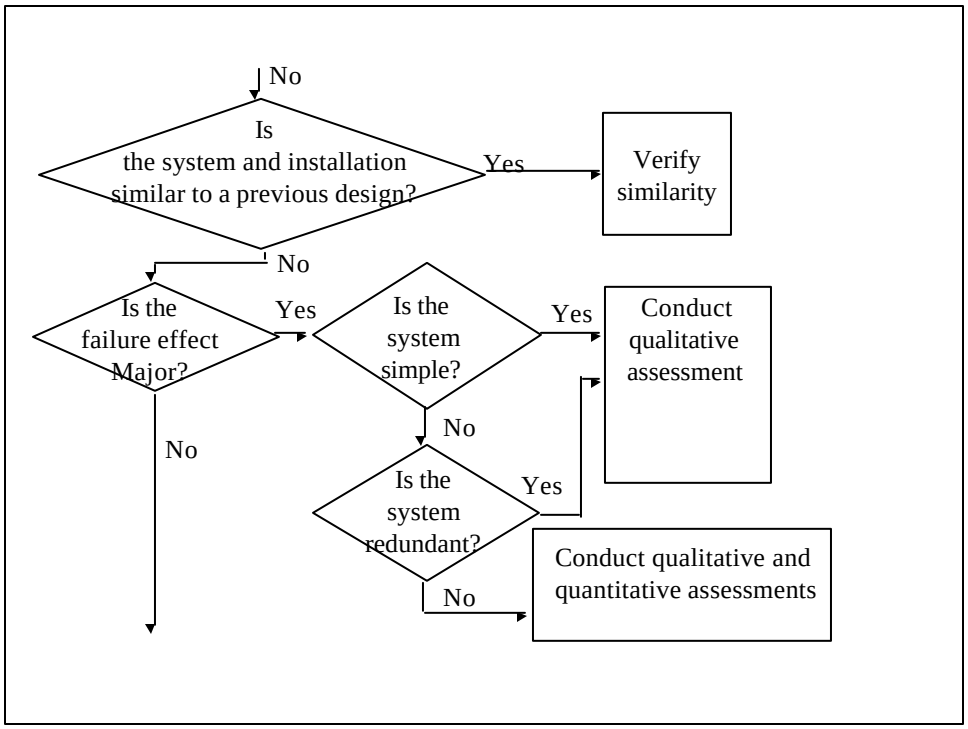
	CATASTROPHIC
Effect on Airplane	Hull Loss
Effect on Occupants	Multiple Fatalities
Effect on Flight Crew	Fatalities or Incapacitation
Qualitative Probability	Extremely Improbable
Quantitative Probability	$< 1.0 \times 10^{-9}$ per flight hour

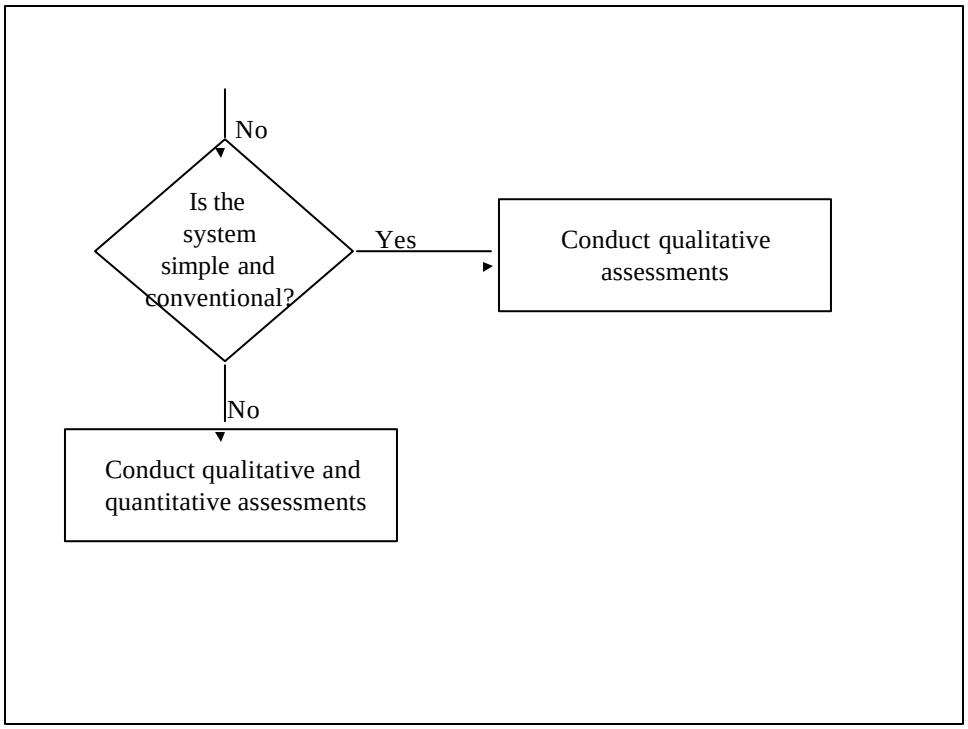
DEPTH OF ANALYSIS

- APPROPRIATE DEPTH OF ANALYSIS IS PRIMARILY BASED ON
  - FAILURE CONDITION CLASSIFICATION
    - CAT, HAZ, MAJ, MIN, NO EFFECT
  - "SIMILARITY"
  - "CONVENTIONALITY"
  - "COMPLEXITY"
- SEE ACTUAL FLOW CHART & TEXT IN AC
- USEFUL TO DISCUSS CASE BY CASE RELATIVELY EARLY IN PROGRAM

DEPTH OF SAFETY ASSESSMENT FLOW CHART




No
Is
the system and installation
similar to a previous design?
Yes
Verify
similarity
No
Is the
failure effect
Major?
Yes
Is the
system
simple?
Yes
Conduct
qualitative
assessment
No
No
Is the
system
redundant?
Yes
Conduct qualitative and
quantitative assessments
No


No
Is the
system
simple and
conventional?
Yes
Conduct qualitative
assessments
No
Conduct qualitative and
quantitative assessments

Where to go for help on Questions of Methodology

Brett Portwood
Technical Specialist for
Safety and Integration
ANM-130L
phone (562) 627-5350
fax (562) 627-5210

Jim Treacy
FAA National Resource Specialist for Avionics
ANM-103N
phone (425) 227-2760
fax (425) 227-1181

Where to go for help on Questions of Methodology concerning Markov Analysis, Fault Trees, Time Limited Dispatch

Hals Larsen
FAA - NRS for Propulsion Controls
Telephone (425) 227-2182
FAX (425) 227-1181

Where to go for help on FAR 25.903 Questions:

MIKE MCRAE ANM-112
Telephone (425) 227-2133
FAX (425) 227-1149

Where to go for help on FAR 25.1309 Questions:

LINH LE, ANM-111
Telephone (425) 227-1105
FAX (425) 227-1320

Where to go for help on FAR 23.1309 Questions

Erv Dvorak, ACE-111
Telephone (816) 329-4123
FAX (816) 329-4091

Phil Petty, ACE-116W
Telephone (316) 946-4139
FAX (316) 946-4407